ต้นฉบับไม่มีหน้า 226-227

No This Page 226-227 In Original

ข้อความตัวจริงออกมาได้ เจ้ากุญแจดังกล่าวนี้เราควรเก็บเอาไว้ในแผ่นดิสเกตต์ เมื่อไหร่ที่เราต้องการใช้ข้อมูลก็ค่อยให้โปรแกรมของเราอ่านเข้าไป โปรแกรมของเรานั้นเมื่อได้กุญแจเข้าไปแล้วก็สามารถอ่านข้อมูลจากไฟล์ แล้วใช้ซับรูทีนถอดรหัสทำการถอดรหัสออกมา โปรแกรมของเราก็จะรู้ข้อมูลจริง และเมื่อจะบันทึกกลับลงจานแม่เหล็กก็ต้องเข้ารหัสเสียก่อน นี่คือขั้นตอนของการใช้ประโยชน์ ลิสติงที่ 2 แสดงตัวอย่างการใช้ประโยชน์จากซับรูทีนทั้ง 2

ลิสติงที่ 2 ตัวอย่างการใช้รูทีนเพื่อเข้ารหัสข้อมูลแล้วเก็บไว้ในไฟล์

```
PROGRAM ENCRYPTION;
LABEL MAINLOOP,EOJ;
TYPE STR8=STRING[8];
     STR80=STRING[80];
TYPE IOTYPE=RECORD
     ENCRYPTEDDATA:STR80;
     END;
VAR IOBUFF:IOTYPE;
VAR ENCRYPTEDFILE:FILE OF IOTYPE;
VAR PLAINTEXT,ENCRYPTEDTEXT:STR80;
VAR ENKEY,CURRENTBLOCK,OUTBLOCK:STR8;
VAR TEXTLENGTH,NOOFBLOCK,K,RECNO:INTEGER;

PROCEDURE ENCRYPT(ENKEY,INWORD:STR8;
                  VAR OUTWORD:STR8);
VAR I,J:INTEGER;
VAR TEMP:ARRAY[1..8] OF CHAR;
VAR CH:CHAR;
BEGIN
  FOR I:=1 TO 8 DO
    BEGIN
    CH:=COPY(ENKEY,I,1);
    J:=ORD(CH)-48;
    TEMP[J]:=COPY(INWORD,I,1);
    END;
  OUTWORD:='';
  FOR I:=1 TO 8 DO
    OUTWORD:=OUTWORD+TEMP[I];
END;

PROCEDURE DECRYPT(ENKEY,INWORD:STR8;
                  VAR OUTWORD:STR8);
VAR I,J:INTEGER;
VAR TEMP:ARRAY[1..8] OF CHAR;
VAR CH:CHAR;
BEGIN
  FOR I:=1 TO 8 DO
    BEGIN
    CH:=COPY(ENKEY,I,1);
    J:=ORD(CH)-48;
    TEMP[I]:=COPY(INWORD,J,1);
    END;
  OUTWORD:='';
  FOR I:=1 TO 8 DO
    OUTWORD:=OUTWORD+TEMP[I];
END;

BEGIN
  ENKEY:='23456781';
  ASSIGN(ENCRYPTEDFILE,'ENCR02.DAT');
  REWRITE(ENCRYPTEDFILE);
  RECNO:=0;

MAINLOOP:
  CLRSCR;
  GOTOXY(1,1);WRITE('PROGRAM TO DEMONSTRATE ENCRYPTION');
  GOTOXY(1,5);WRITE('   PLEASE ENTER PLAINTEXT:      ');
  GOTOXY(1,6);WRITE('   <ENTER END TO END JOB>       ');
  GOTOXY(1,8);READ(PLAINTEXT);
  IF PLAINTEXT='END' THEN GOTO EOJ;
  GOTOXY(1,10);WRITE('       PLAINTEXT=',PLAINTEXT);
```

(ต่อ)

ลิสติงที่ 2 (ต่อ)

```
  TEXTLENGTH:=LENGTH(PLAINTEXT);
  NOOFBLOCK:=TEXTLENGTH DIV 8;
  IF 8*NOOFBLOCK<TEXTLENGTH THEN
    BEGIN
    NOOFBLOCK:=NOOFBLOCK+1;
    FOR K:=TEXTLENGTH+1 TO 8*NOOFBLOCK DO
      PLAINTEXT:=PLAINTEXT+' ';
    END;
  ENCRYPTEDTEXT:='';
  FOR K:=1 TO NOOFBLOCK DO
    BEGIN
    CURRENTBLOCK:=COPY(PLAINTEXT,8*(K-1)+1,8);
    ENCRYPT(ENKEY,CURRENTBLOCK,OUTBLOCK);
    ENCRYPTEDTEXT:=ENCRYPTEDTEXT+OUTBLOCK;
    END;
  GOTOXY(1,11);WRITE('  ENCRYPTEDTEXT=',ENCRYPTEDTEXT);
  SEEK(ENCRYPTEDFILE,RECNO);
  IOBUFF.ENCRYPTEDDATA:=ENCRYPTEDTEXT;
  WRITE(ENCRYPTEDFILE,IOBUFF);
  GOTOXY(1,24);WRITE('ANY KEY TO CONTINUE');
  REPEAT UNTIL KEYPRESSED;
  GOTO MAINLOOP;

EOJ:
  CLOSE(ENCRYPTEDFILE);
  GOTOXY(1,24);WRITE('END OF JOB          ');
END.
```

■

ดูแล้วง่าย จริงไหม ไม่แน่เสมอไปหรอกครับ เรายังไม่ได้ลงในรายละเอียดอยู่อีก 3 - 4 เรื่อง เรื่องแรกก็คือ เราจะสร้างกุญแจขึ้นมาได้อย่างไร? มันมีกฎเกณฑ์หรือข้อพึงระวังอย่างไรบ้าง? เรื่องที่ 2 คือ เราควรจะใช้ความยาวของข้อมูลเป็นท่อนละเท่าใดแน่? เรื่องที่ 3 คือ เจ้าบล็อกสุดท้ายของข้อมูลที่เราตัดออกเป็นท่อน ๆ นั้นจะมีตัวอักษรจริงอยู่ไม่กี่ตัว เมื่อเราเอา "space" มาเติมแล้วเข้ารหัสโดยโยกย้ายไปมามันก็จะยังมองเห็นตัวอักษรตัวจริงอยู่เท่าเดิม ซึ่งจะทำให้ผู้ร้ายพอจะเดาได้ เรื่องนี้เราจะปรับปรุงหรือแก้ไขได้อย่างไร เรื่องสุดท้ายก็คงจะเป็นคำถามว่า เราควรเปลี่ยนกุญแจบ่อยสักแค่ไหน

กฎเกณฑ์การสร้างกุญแจ

เรามาดูเรื่องกฎเกณฑ์ในการสร้างกุญแจกันเสียก่อน กฎที่สำคัญมี 3 ข้อ คือ

1. ควรให้มีการโยกย้ายทุกตำแหน่ง
2. อย่าให้มีแพตเทอร์น
3. โยกย้ายลงในตำแหน่งที่ซ้ำกันไม่ได้

กฎข้อแรกนั้นมีไว้เพื่อให้ยากต่อการค้นหากุญแจ กฎข้อนี้อาจไม่จำเป็นต้องยึดถือ 100 เปอร์เซ็นต์ หรือในภาษาฝรั่งเขาเรียกว่า "Not necessary, but recommended" ยกตัวอย่างเช่น ถ้าเราโยกย้าย 7 ตัว ก็จะมีผลทำให้ข้อความเดิมนั้นอ่านไม่ออกเท่า ๆ กับการย้ายครบทั้ง 8 ตัวอักษร แต่ถ้าเราโยกย้ายเพียง 2 - 3 ตัวอักษร ส่วนที่เหลืออยู่อีก 5 - 6 ตัวอักษรนั้น อาจมองเห็นเป็นคำในภาษาไทยหรือภาษาอังกฤษได้ หลังจากที่ผู้ร้ายรู้ว่าตัวอักษรใดบ้างที่ไม่มีการโยกย้ายเขาก็จะเดาส่วนที่เหลืออยู่ได้โดยง่าย ดังนั้นผมจึงแนะนำควรปฏิบัติตามข้อ 1. เสียหน่อย

สำหรับกฎเกณฑ์ข้อ 2. นั้นก็เข้าลักษณะเป็นกฎเกณฑ์ที่ไม่จำเป็นต้องยึดถือ 100 เปอร์เซ็นต์ มันช่วยแค่ป้องกันไม่ให้ผู้ร้ายแกะหากุญแจได้โดยง่ายเช่นกัน ยกตัวอย่างเช่น ในรหัส "23456781" ที่ยกขึ้นมาเป็นตัวอย่างนั้นมีแพตเทอร์นที่เด่นชัด คือเป็นการเคลื่อนย้ายไป 1 ตำแหน่งถัดไป ส่วนตัวอักษรตัวสุดท้ายก็ถูกเตะวนมาอยู่หน้าสุด กุญแจแบบนี้ทำให้ข้อความส่วนใหญ่ยังอ่านออก วิธีที่จะทำให้ไม่มีแพตเทอร์นก็คืออย่าคิดเอาเอง เราจะต้องใช้เครื่องคอมพิวเตอร์เข้าช่วย เครื่องสามารถสร้างตัวเลขสุ่ม (Random Numbers) ให้เรา เราเอาเลขสุ่มเหล่านี้เป็นตัวบอกว่าดิจิตต่าง ๆ ของกุญแจควรมีค่าเป็นเท่าใด เมื่อได้กุญแจออกมาแล้วก็ควรวิเคราะห์ด้วยสายตาเสียหน่อยว่ามันมีลักษณะที่เป็นกฎเกณฑ์ง่าย ๆ หรือไม่ แต่ส่วนใหญ่แล้วสิ่งที่เครื่องคอมพิวเตอร์สร้างให้นั้นมันมักจะไม่มีแพตเทอร์นอะไรให้เห็น

กฎเกณฑ์ข้อ 3. นั้นเป็นกฎเกณฑ์ที่จำเป็นต้องปฏิบัติตาม ทั้งนี้เพราะถ้าเราไปย้ายตัวอักษร 2 ตัว ลงไปในที่เดียวกัน ก็จะเกิดการทับกับ ตัวอักษรที่ถูกย้ายลงไปก่อนก็จะหายไป ถึงเวลาถอดรหัสแล้วเราจะ

ต้นฉบับไม่มีหน้า 230-231

No This Page 230-231 In Original